APPARATUS AND METHOD FOR EFFICIENTLY RUNNING APPLICATIONS ON A WIRELESS COMMUNCATION DEVICE

BACKGROUND

FIELD

[01] The present invention relates generally to communications, and more specifically, to the transmission of data over wireless communication systems.

BACKGROUND

[02] Various domestic and international standards have been established for the over-the-air interfaces associated with cellular telephone systems, each system being based upon multiple access techniques such as frequency division multiple access (FDMA), time division multiple access (TDMA), or code division multiple access (CDMA). Some of the more well-known of these standards are Advanced Mobile Phone Service (AMPS), Global System for Mobile (GSM), and Interim Standard 95 (IS-95). IS-95 and its derivatives, IS-95A, IS-95B, ANSI J-STD-008 (referred to collectively herein as IS-95), and other high-data-rate systems are promulgated by the Telecommunication Industry Association (TIA) and like standards bodies. Cellular systems, as used herein, includes cellular and personal communications services (PCS) frequencies.

[03] IS-95 cellular telephone systems use CDMA signal processing techniques to provide efficient and robust cellular telephone service. Cellular telephone systems configured substantially in accordance with the use of the IS-95 standard are described in U.S. Patent Nos. 5,103,459 and 4,901,307, which are assigned to the assignee of the present invention and are incorporated by reference herein. CDMA techniques are also used in the cdma2000 ITU-R Radio Transmission Technology (RTT) Candidate Submission (referred to herein as cdma2000), issued by the TIA. The standard for cdma2000 is given in the draft versions of IS-2000 and IS-856 (cdma2000 1xEV-DO). The cdma2000 1xEV-DO communication system defines a set of data rates, ranging from 38.4 kbps to 2.4 Mbps, at which a base station (BS) may communicate with a wireless communication device.

[04] Given the growing demand for wireless data applications, the need for very efficient wireless data communication systems has become increasingly significant. In particular, as computer users have become increasingly mobile, the need has arisen to access the internet protocol (IP) network via the wireless networks on an efficient and high-speed basis. IP network access may be provided through a wireless network by tethering a wireless communication device to an electronic computing device, the tether comprising either a physical or wireless connection. The electronic computing device is referred to hereinafter as terminal equipment (TE). Applicable wireless communication devices are also referred to as "mobile stations" (MS) or "user equipment" (UE) in some of the wireless communication standards. For illustrative ease, the terminology "MS" will be used hereinafter. A MS may be, for example, a cellular phone, a personal digital assistant (PDA), a wireless modem, combinations thereof, or the like. A TE may be a computing device, such as, for example, a laptop computer, a desktop computer, a PDA, or combinations thereof. The wireless or physical medium between a MS and TE may include one or more PCMCIA cards, Universal Serial Bus (USB) media, serial media, BlueTooth, IEEE 802.11, or the like. The wireless medium between the MS and the TE, and between the MS and the network, may perform transmission of data packets that originate or terminate at points within an IP network.

[05] A myriad of protocols exist for transmitting packetized traffic between points within IP networks, so that information arrives at its intended destination. A principal such protocol is "The Internet Protocol," Request for Comment (RFC) 791 (September, 1981). The IP protocol requires that each data packet begins with an IP header containing source and destination address fields that uniquely identify host and destination points. Addresses for destination points and source points are differentiated by the unique IP address in a header portion of each data packet. The IP protocol provides for the fragmentation of large data packets into a train of smaller packets before transmission, so that a destination point must be able to reassemble the large packet from the smaller packets upon receipt of the destination IP address fields of the smaller packets. The most recent version of the IP protocol is IPv6. IPv6 uses larger IP address lengths (128 bits as compared to the 32 bits that was standardized in the old protocol, IPv4), and thus can support more devices on the network. Another protocol is "IP Mobility Support," promulgated in RFC 2002 (October 1996), which is a protocol that provides for transparent routing of IP datagrams to mobile nodes.

[06] The Point-to-Point Protocol (PPP), promulgated in RFC 1661 (July 1994), provides a standard method in the link layer of a communication for encapsulating IP information over point-to-point links. As such, PPP provides for the use of Transmission Control Protocol/Internet Protocol (TCP/IP) networking applications at and among points on a network. TCP/IP is the collection of networking protocols that provide a framework used by applications to communicate information over a network. TCP/IP includes IP protocol in the network layer of a communication and TCP protocol in the transport layer of a communication. IP is the central, unifying protocol in TCP/IP, and as such, provides the basic delivery mechanism for packets of data sent between all points on a network.

[07] The Transmission Control Protocol (TCP) provides a reliable transfer between two points on a network. TCP assures data integrity by assuring the ordered and complete delivery of data. TCP depends on IP to move packets from point to point on the network. TCP establishes and ends a connection with the destination IP address via an exchange of management packets. Each application running TCP distinguishes itself from other applications at the same network point by reserving a 16-bit port number. Port numbers are placed in the TCP header by the originator of the packet before the packet is passed to the network, and the destination port number allows the IP packet to be delivered to the intended recipient at the destination point.

[08] In the communication protocols discussed hereinabove, and particularly in PPP, data is sent over slow serial links. Compression was designed to alleviate this slowness. More specifically, because the point-to-point efficiency of a protocol is related to the ratio of data to the entire packet (including header information and data) sent over the serial line, header compression is motivated by the need for improved interactive response over serial lines.

[09] Van Jacobson header compression (VJ compression) was designed to compress the header transmission of TCP/IP. Each TCP/IP packet has a header, normally 40 bytes in length. Of these 40 bytes, 20 bytes are normally assigned to IP fields and 20 bytes are normally assigned to TCP fields. Van Jacobson compression reduces the size of a TCP/IP header to as few as three bytes.

[10] The initial TCP/IP header sent for a TCP/IP session contains the necessary information to exchange the IP packet with the right destination, and to exchange data with the right port at the right destination, for a given TCP/IP session. However, once

an initial header is received and the session is established, the end points of the TCP/IP session over the PPP need only be informed of which session the incoming TCP/IP is associated with, because the remainder of the addressing fields in the header remain static for the duration of the session. Thus, most of the static addressing fields needed in the initial TCP/IP header can be eliminated in subsequent headers for that session. The elimination of these static header fields after receipt of the initial uncompressed TCP/IP header constitutes the VJ compression of the subsequent TCP/IP headers.

[11] Note that an IP packet is a non-TCP/IP packet, or an uncompressable TCP/IP packet, in accordance with RFC 1144 (February 1990). A VJ uncompressed packet is similar to an IP packet, but has a connection identification (CID) replacing the IP protocol field in the IP packet. A VJ compressed packet has a VJ compressed header, but also includes a CID. The CID is used to identify the connection at a source from which a communication originated, or at a destination to which information is targeted. As such, the CID may represent the respective ports through which sending application software and receiving application software communicate. Due to the fact that a sending port and a receiving port can track an active communication once that communication is originated, subsequent TCP/IP packets after the originating TCP/IP packet need only send a CID to the destination rather than detailed addressing information. This use of the CID is enabled because the sender and receiver retain the original detailed addressing information from the originating IP packet for the duration of the communication link, and thus can send communications to the correct destination using only the short-hand of the CID.

[12] The transmission of data packets using compression from the IP network over a wireless communication network, or from the wireless communication network over the IP network, is allowed by adherence to a set of protocols. This set of protocols is referred to as a protocol stack. A MS may be the origination or the destination of an IP packet, or the MS may be a gateway to an electronic device that is the origination or destination of an IP packet.

[13] IP packets are transported between the wireless communication network and an IP network destination via a packet data service node (PDSN) in the wireless communication network that provides access to the IP network. The TCP/IP header in non-initial communications through the PDSN is often VJ compressed. The VJ

compressed TCP/IP header and the accompanying TCP/IP packet data are embedded as part of the data of the PPP packet.

[14] An MS typically has more limited computing power than a stationary electronic device due, in part, to hardware and size restrictions. Running software applications on both the MS and the TE, while the MS and TE share the MS as the gateway to the wireless network and the IP network, also causes severe computing limitations. Thus, it would be desirable, in order to minimize the computing necessary at the MS which serves as the gateway to the wireless and IP networks, to provide an efficient way for an MS to detect whether an incoming packet is an IP packet. Likewise, it would be desirable for the MS to detect whether a TCP/IP packet header is VJ compressed or VJ uncompressed and, if the incoming packet header is VJ compressed, to assess the destination of the incoming packet without uncompressing the VJ compressed header.

[15] Therefore, the need exists for an apparatus, system and method that improves the efficiency of the MS in filtering VJ compressed TCP/IP headers, and improves the efficiency of the MS in assessing the destination of IP packets.

BRIEF SUMMARY

[16] In one aspect of the invention, a snooper is presented for efficiently processing at least one packet incoming to a mobile station. The snooper includes a receiver for receiving VJ compressed ones of the at least one packet; a storage, communicatively associated with the receiver, for storing at least one list, wherein the at least one list includes at least one connection identification of at least one of an active originator and an active destination for ones of the at least one packet; and a comparator for delineating a received connection identification of one of the VJ compressed ones of the at least one packet received at the receiver against the at least one list.

[17] In another aspect, a filter is presented for efficiently processing at least one packet incoming to a mobile station. The filter includes a receiver for receiving IP ones and VJ uncompressed ones of the at least one packet; a delineator for delineating the IP ones from the VJ uncompressed ones of the packets, wherein the delineator seeks a connection identification in a one of the VJ uncompressed packets upon delineation of the one of the VJ uncompressed packets as destined for the mobile station, and wherein the delineator forwards the connection identification to a connection identification list

for subsequently assessing a destination of at least one VJ compressed packet associated with the one of the VJ uncompressed packets.

[18] In another aspect, a method is presented for efficiently processing at least one packet incoming to a mobile station. The method includes receiving VJ compressed ones of the at least one packet; storing at least one list, wherein the at least one list includes at least one connection identification of at least one of an active originator and an active destination for ones of the at least one packet; and comparing a received connection identification of one of the VJ compressed ones of the at least one packet against the at least one list.

[19] In another aspect, a method is presented for efficiently filtering at least one packet incoming to a mobile station. The method includes receiving IP ones and VJ uncompressed ones of the at least one packet; delineating the IP ones from the VJ uncompressed ones of the IP packets; seeking a connection identification in a one of the VJ uncompressed packets upon delineating of the one of the VJ uncompressed packets as destined for the mobile station; and forwarding the connection identification to a connection identification list.

[20] In another aspect, a system is presented for efficiently processing at least one packet incoming to a mobile station. The system includes a mobile station; a filter resident on the mobile station that differentiates IP ones of the at least one packet and VJ uncompressed ones of the at least one packet; at least one PDSN in communication with the mobile station; at least one terminal equipment communicatively tethered to the mobile station; at least one snooper on the mobile station, wherein the snooper receives at least one VJ compressed packet incoming to the mobile station from at least one of the PDSN and the terminal equipment, wherein the at least one VJ compressed packet is compared by the snooper to at least one list that includes at least one connection identification of at least one of an active originator and an active destination for ones of the at least one packet, wherein the active destination is resident at at least one of the terminal equipment and a site associated with the PDSN; and at least one connection local to the mobile station for receiving the at least one VJ compressed packet having the connection identifier that matches the at least one list.

[21] In another aspect, a snooper is presented for efficiently processing at least one Internet Protocol (IP) packet incoming to a mobile station, comprising: at least one storage element for storing at least one list of Van Jacobson (VJ) connection

identifications (CID), each VJ CID associated with an active application running on the mobile station; and a processing element configured to delineate between a packet with a VJ CID and a packet without a VJ CID, and if the packet has a VJ CID, to compare the VJ CID against the entries of the at least one list.

[22] Thus, the present invention provides apparatus, systems and methods that improve the efficiency of the MS in filtering VJ compressed TCP/IP headers, and improve the efficiency of the MS in assessing the destination of IP packets having VJ compressed TCP/IP headers without uncompressing the VJ compressed TCP/IP headers of such IP packets..

BRIEF DESCRIPTION OF THE DRAWINGS

[23] The disclosure herein will be described in greater detail with reference to the following drawings, wherein like reference numerals designate like elements, and wherein:

[24] Figure 1 is a block diagram of the interaction of an MS, a wireless network, and an IP network;

[25] Figure 2 is a block diagram illustrating a system of accessing, by a mobile computing device, of a networked connection;

[26] Figure 3 is a flow diagram illustrating a method by which a mobile computing device may access information;

[27] Figure 4 is a flow diagram illustrating a method of filtering and snooping TCP/IP packets; and

[28] Figure 5 is a state diagram illustrating a filter and a snooper.

DETAILED DESCRIPTION

[29] It is to be understood that the figures and descriptions herein have been simplified to illustrate elements that are relevant for a clear understanding of the discussion herein, while eliminating, for purposes of clarity, many other elements found in a typical network communication apparatus, system and method. But because such elements are well known in the art, and because they do not facilitate a better understanding of the discussion herein, a discussion of such elements is not provided herein. The disclosure herein is directed to all such variations and modifications to the

applications, networks, and systems disclosed herein and as will be known, or apparent, to those skilled in the art.

[30] Figure 1 illustrates the connections between a plurality of mobile stations (MS) and various infrastructure elements of two CDMA-based systems. A plurality of MSs 10a-b operates within sectors of a plurality of base station controllers (BSCs) 20a-c, 20d-e, 20f-h of different networks 5a, 5b. The BSCs 20a-c, 20d-e, 20f-h are supported by packet control functions (PCF) 30a, 30b, 30c, respectively. Some PCFs 30a, 30b are supported by a PDSN 40a of one network 5a, while other PCFs 30c are supported by a PDSN 40b of another network 5b. It should be understood by one of skill in the art that there could be any number of MS 10, BSC 20, PCF 30 and PDSN 40 elements. The PDSNs 40a, 40b are coupled to an IP or private network 50, which is coupled to a Home Agent 70 of the MSs 10.

[31] MS 10 may be any of a number of different types of wireless communication devices such as a portable phone, a cellular telephone, a cellular telephone that is connected to a laptop computer running IP-based applications, a cellular telephone with associated hands-free car kit, a personal data assistant (PDA) running IP-based applications, a wireless communication module incorporated into a portable computer, or a fixed location communication module such as might be found in a wireless local loop or meter reading system.

[32] A "handoff" occurs when a MS moves from the support of one base station to the support of another base station. Handoffs may be "soft," wherein the device is in communication with both base stations at the same time during the handoff process, or "hard," wherein the device ends communications with one base station before beginning communications with another base station. A handoff between one CDMA air interface system and another air interface system is referred to as a "dormant" handoff when a data session is connected, but not active. In other words, the MS and the PDSN maintain the PPP state but do not transfer data in a dormant handoff. When the MS is actively transferring to a PDSN, then the session is referred to as an "active data session."

[33] A MS may be tethered to one or more terminal equipment devices (TE), and the MS may provide access to an IP network via the wireless network. The MS may

provide a gateway for the TE to send and receive TCP/IP packets along the IP network via the wireless network.

[34] The TCP/IP includes a header detailing the specifics of the TCP/IP packet data correspondent to that header. The TCP/IP header may be Van Jacobson (VJ) compressed in order to improve communication efficiencies, particularly over the limited bandwidth connection of the MS to the wireless network.

[35] The travel of TCP/IP packets between the wireless network and the IP network is inefficient because the MS uncompresses all TCP/IP packets having VJ compressed headers incoming to the MS. The MS uncompresses the VJ compressed headers in order to assess whether the TCP/IP packets are destined for the MS or for the TE that is tethered to the MS. The embodiments described herein illustrate a filter that improves computing efficiency for a MS that is used as a gateway for a TE by, among other things, directing incoming TCP/IP packets having VJ uncompressed headers to the correct destination. The embodiments described herein also illustrate a snooper that distinguishes and selects IP packets having VJ compressed headers for uncompressing at the MS, and forwards those packets with VJ compressed headers that are not destined for the MS to the TE without uncompressing.

[36] It will be apparent to those skilled in the art in light of the disclosure herein that the present systems and methods may be employed not only in a CDMA2000 network, but also in an Universal Mobile Telecommunications System (UMTS) network, or any other network in which a single IP address is assigned for both the MS and the TE.

[37] Figure 2 is a block diagram illustrating a system and apparatus 100 for accessing a wireless network 5 by terminal equipment (TE) 112 via the MS 10. The wireless network 5 is connected, via a PDSN 40, to an IP network 50. The system includes a TE 112 running one or more TE applications 120. Applications, as used herein, include one or more computer software programs that perform one or more computing functions. As used herein, MS applications 134 are run by at least one processor at the MS 10, and TE applications 120 are run by at least one processor at the TE 112. At least one of the TE applications 120 exchanges IP packets, via the MS 10 and the wireless network 5, with the IP network 50.

[38] One or more of the TE applications 120 may request access to information available on the IP network 50, such as the Global Positioning System (GPS) coordinates of the TE 112. This request, and the responsive information to the request,

pass through the IP network 50 and, via the PDSN 40, over the wireless network 5, to and from the MS 10. The MS 10 then must communicate the information to and from the TE 112. Such an information request may overlap other information requests from the TE 112 passed over the same medium 116 to the MS 10. The medium 116 between the MS 10 and the TE 112 may be a wireless or wired medium, such as one or more PCMCIA cards, USB media, serial media, BlueTooth, IEEE 802.11, or the like. The communication over the medium 116 may be a PPP based connection, an Ethernet-like connection, or any type of IP protocol connection.

[39] The TE applications 120 may be applications running TCP/IP, and may request GPS coordinates from the IP network 50. It will be apparent to those skilled in the art that the discussion herein is not restricted to GPS requests, but can be similarly employed for any TE application 120 running TCP/IP.

[40] The MS 10 may be any device capable of connecting the tethered TE 112 to a wireless network 5. The MS 10 may include one or more receivers 144 for receiving data. The MS 10 provides a gateway, via the wireless network 5, to the IP network 50 to which the TE applications 120 send and receive IP packets. The MS 10 passes IP packets and TCP/IP packets outgoing from the TE 112 to the wireless network 5 for entry to the IP network 50 via the PDSN 40. The MS 10 receives IP packets sent from the IP network 50, via the PDSN 40, over the wireless network 5. The MS 10 may have running thereon one or more MS applications 134. The MS applications 134 may run TCP/IP. The MS applications 134 may send and receive IP packets from the IP network 50 via the wireless network 5. Thus, both the TE applications 120 and the MS applications 134 may receive IP packets via the MS 10 from the IP network 50 over the wireless network 5.

[41] Certain IP packets incoming to the MS from the IP network may be destined for the MS applications, and other packets incoming to the MS from the IP network may be destined for the TE applications. By virtue of MS hardware dedicated to MS applications running on the MS and to MS hardware dedicated to the transmission and reception of communications over the wireless network, the MS may have limited computing power remaining for processing IP packets. In order to alleviate unnecessary computing by the MS, such as computing on packets destined for TE applications, the MS may include at least one snooper 140 to delineate the destination of VJ compressed packets, and more specifically to delineate whether TCP/IP packets having VJ

compressed headers are destined for an MS application or a TE application. As used herein, a delineator may view, identify, separate, differentiate, or any combination thereof, packetized data. In order to further alleviate unnecessary computing for the MS, the MS may include at least one filter 138 to delineate types and destinations of packets, based on packet headers of packets incoming to the MS.

[42] Each filter may pass TCP/IP packets having VJ uncompressed headers, and IP packets, to the destination of the packet. The filter may be one or more software programs, and the software programs may be associated with hardware within the MS. The filter delineates the destination of the packets incoming to the MS. The destination, according to the header of the packet, is the TE or the MS. The destination of a VJ uncompressed header TCP/IP packet is denoted by a connection identification (CID). Upon receiving a TCP/IP packet having a VJ uncompressed header, the filter assesses whether a CID list maintained at the MS includes that particular CID as correspondent to an active MS application or an active TE application. The filter then directs the IP packet to the correct destination. If the CID of a VJ uncompressed TCP/IP packet is not on the CID list, the filter may determine that the unknown CIP should be added to the CID list.

[43] A snooper may be one or more software programs, and the software programs may be associated with hardware within the MS. The software programs of the snooper are preferably capable of checking TCP/IP headers of TCP/IP packets for, among other information, VJ compression information and CID information. Each snooper further includes storage for storing at least one CID list of applications active at either the TE or the MS.

[44] Each snooper receives packet information incoming to the MS from the IP network and delineates IP packets having VJ compressed headers. The filter differentiates between IP packets with VJ uncompressed headers and IP packets without either VJ uncompressed or VJ compressed headers. For IP packets without either VJ compressed or uncompressed headers, the filter may delineate by assessing and assigning the destination of that IP packet. If the destination of that IP packet is at the MS, and the destination assessed is not on the CID list, the snooper may be alerted to snoop for the incoming VJ uncompressed packets that follow.

[45] The snooper views the CID of VJ compressed headers incoming to the snooper. The snooper includes a CID list. The CID list may include CIDs having active TCP/IP

sessions, or alternatively, having the capability for TCP/IP sessions, at either the MS or at the TE. Thus, the CID list may be limited to CIDs for running MS applications. Alternatively, the CID list may be limited to running TE applications. The CID of the VJ compressed header is compared, such as by comparator 156, against the CID list in the snooper, and action is taken by the snooper to forward the packet to the destination application 120, 134 according to the outcome of the comparison against the CID list. If the CID list includes running TCP/IP MS applications, and the CID to which the TCP/IP packet having the VJ compressed header is directed is the port of a running MS application on the CID list, the header is VJ uncompressed and sent to the destination, i.e. the port of that MS application. If the CID to which the TCP/IP packet having the VJ compressed header is not directed to a running MS application on the CID list, that packet is forwarded, without uncompressing, to the destination according to the CID. Typically, that destination is the TE.

[46] Thus, the snooper allows for an avoidance of the step of uncompressing the headers of all TCP/IP packets incoming to the MS having VJ compressed headers. Rather, the snooper delineates only those TCP/IP packets having VJ compressed headers that are destined for running MS applications, which are then uncompressed. This delineation, in an embodiment wherein the CID list includes only running MS applications, includes identifying those CIDs on the CID list and uncompressing the header of only those IP packets destined for the MS applications.

[47] Certain of the packets sent from the TE may be destined for the MS. Thus, the delineations performed by the filter and snooper may also delineate the destination, based on the source CID, of packets incoming to the MS from the TE. If a TCP/IP packet having a VJ compressed header is destined for a running MS application from a CID at the TE on the source CID list, the MS may uncompress the header of such packets and pass those uncompressed packets to the internal stack of the MS for use by the running MS application destination. Otherwise, the TCP/IP packet having VJ compressed header is forwarded from the MS over the wireless network to the PDSN.

[48] Likewise, if the destination of the TCP/IP packet having VJ uncompressed header from the TE is at the MS, that source CID at the TE may be added to the CID list as an active source for the MS, and snooping may begin for VJ compressed packets from the same source CID at the TE to the MS. If the destination of the TCP/IP packet

having VJ uncompressed header is not at the MS, the packet may be forwarded from the MS over the wireless network to the PDSN.

[49] In general, a majority of the packets from the wireless network to an MS which is tethered to a TE are destined for the running TE applications. Hence, by snooping and filtering to delineate only those packets destined for MS applications, processing efficiency is greatly improved at the MS.

[50] In Figure 3, a TE application may request, from the IP network, the GPS position of the TE. In order to obtain the GPS position information, a TE application may make a GPS location request to an IP address, using TCP/IP, through the MS over the wireless network and the IP network 202. The site at that IP address may respond by assessing the location of the MS, such as by methods known in the art, and by sending the location of the MS, in a TCP/IP packet, over the IP network, through the PDSN to the wireless network, over the wireless network to the MS, and through the gateway provided by the MS to the TE 204. If the TCP/IP packet that includes the requested GPS information has a VJ uncompressed header, the MS may route the TCP/IP packet of GPS information to the destination at the TE 208 via the filter 300. If the TCP/IP packet that includes the requested GPS information has a VJ compressed header, the MS may route the IP packet of GPS information to the destination at the TE via the snooper 300, without uncompressing the TCP/IP packet header.

[51] A single IP address may be shared by all applications on the TE and the MS that are accessing the particular PDSN. In order to alleviate this difficulty, an artificial IP address may be assigned to the TE by the filter. For example, the artificial IP address may be assigned as 10.10.10, or a like IP address, that is not used globally on the IP network. In the example of a GPS request from the TE, the outgoing GPS request from the TE which is destined for a site on the IP network may be designated by the MS as originating from the artificial IP address assigned to the TE by the MS. The GPS information regarding the location of the MS IP address may be returned from the IP network to the MS IP address as the GPS location of the MS, but the GPS information may actually be destined, as tracked by the filter, for the artificial IP address of the TE as the originator of the request. The filter may note the artificial IP address as being on the CID list and as being requested information, and the filter or the snooper may accordingly forward the GPS information to the TE upon receipt.

[52] Figure 4 is a flow diagram illustrating an embodiment of the snooping and filtering discussed herein. In this embodiment, the MS may continuously, or selectively, snoop and filter on the packets incoming to the MS.

[53] To unframe and process only those packets destined for a running MS application, the snooper and filter delineate which packets are destined for MS applications. For TCP/IP packets having VJ compressed headers, the first TCP/IP packet that initiates the communication cannot include a VJ compressed header. Thus, if a series of TCP/IP packets having VJ compressed headers are preceded by a TCP/IP packet that has a VJ uncompressed header assessed by the filter as destined for the MS, those TCP/IP packets having VJ compressed headers are snooped by the snooper as destined for the MS. Receipt of that first VJ uncompressed packet destined for an MS application causes the filter to add the CID of that MS application to the CID list, and starts the snooper snooping for IP packets having VJ compressed headers destined for that CID. Received TCP/IP packets having VJ compressed headers and not having a CID on the CID list, are forwarded to the TE.

[54] Once a CID is added to the CID list, the snooper recognizes that outgoing TCP/IP packets having VJ compressed headers may be expected to eminate from that CID. Since the source CID of such an outgoing communication may be compressed, the CID list continuously or at intervals tracks current CIDs in use, by either the TE applications or the MS applications, and may retain those active CIDs on the CID list until communication by that CID is affirmatively terminated. Upon termination of the TCP/IP communication for a CID, the MS may no longer snoop for that CID, but rather, may return to filtering for VJ uncompressed packets for that CID.

[55] As illustrated in Figure 4, an incoming packet may be assessed by the filter as to packet type 302, namely as an IP packet, a TCP/IP packet having a VJ uncompressed header, or a TCP/IP packet having a VJ compressed header. Non-TCP packets and uncompressible TCP packets constitute IP packets. A VJ uncompressed TCP/IP packet is an IP packet with the IP protocol field replaced with the CID. A VJ compressed TCP/IP packet includes a compressed TCP/IP header and the CID.

[56] If the packet is a TCP/IP packet having a VJ compressed header 304, the CID of the packet is checked against the snooper CID list 306, 308, and the packet is forwarded to the TE if the CID is for a TE application, i.e. not for an MS application on the CID

list. If the VJ compressed packet is destined, according to the CID list comparison, for an MS application, the packet is forwarded to the internal stack of the MS 312.

[57] If a TCP/IP packet having a VJ uncompressed header is received 316, a destination CID is assessed 318, 320 by the filter. If the destination CID is not at the MS, the packet is forwarded to the TE 310. If the packet is for inclusion on the internal stack of the MS 324, i.e. is directed to a CID of an MS application, that CID is added to the CID list to allow the snooper to snoop all incoming IP packets 330 for that CID. If the packet is not for inclusion on the internal stack of the MS, the packet is forwarded by the filter to the TE 310.

[58] If an IP packet is received 334, the destination of the IP packet is assessed 336, and that destination is checked for inclusion on the MS stack 338. An IP packet not for inclusion on the MS stack is forwarded to the TE 310. If the IP packet is for inclusion on the MS stack, the packet is checked for status as a TCP/IP communication 340. If the packet is a TCP/IP communication, the packet is checked for direction to an MS application 340. If the packet is directed to an MS application that is active of record, such as on the CID list 350, 352, the packet is passed up the internal stack of the MS 312. If the packet is directed to an MS application that is not active of record, and if the CID list does not include that MS application 350, 352, that packet is passed up the internal stack of the MS 312, and the snooper begins snooping for incoming TCP/IP packets having VJ uncompressed headers destined for the CID correspondent to that MS application 354. That CID may then be added to the CID list, because, if an initializing TCP/IP packet having a VJ uncompressed header arrives and is destined to that CID, additional packets having VJ compressed headers can be anticipated to and from that CID.

[59] Figure 5 is a state diagram 400 illustrating the actions of a snooper and a filter. As illustrated, and in accordance with the flow of Figure 4, if no applications are running, the snooper and filter take no action 402. State 402 is the default and reset state, which occurs before IP packet communications or upon termination of TCP/IP communication by CIDs on the CID list.

[60] If the filter receives a VJ uncompressed packet 404, the filter assesses whether the packet is destined for an MS application. If the packet is destined for an MS application, the CID of that packet is added to the CID list, and the snooper 408 is started to snoop for subsequent packets destined for that CID.

[61] If the filter receives an IP packet not having a VJ compressed header or a VJ uncompressed header, the snooper 408 is set to snoop for VJ uncompressed packets which provide a CID as the destination for packets subsequent to that IP packet 406. That CID is added to the CID list upon receipt of the first VJ uncompressed packet, and VJ compressed packets directed to that CID may then be snooped for uncompression and direction to MS applications, if the CID list includes active MS applications.

[62] Those of skill will appreciate that the various illustrative logical blocks, modules, circuits, and steps described in connection with the disclosure herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[63] The various illustrative logical blocks, modules, and circuits described herein may be implemented or performed with a processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A processor may be a microprocessor, or any conventional processor, controller, microcontroller, or state machine. A processor may be a combination of such computing devices.

[64] The steps described herein may be embodied in hardware, in a software module executed by a processor, or in a combination thereof. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor. In the alternative, the storage medium may be integral to the processor.

[65] If not otherwise stated herein, it may be assumed that all components and processes described herein may, if appropriate, be considered to be interchangeable with similar components and processes disclosed elsewhere in the specification or known to

those skilled in the art. The embodiments described hereinabove are thus to be considered, in all respects, as illustrative and not restrictive. All that comes within the meaning and range, and within the equivalents, of the claims hereinbelow is therefore to be embraced within the scope thereof.

What is claimed is: